REMARKS

This paper responds to the first Office action, which was non-final.

Claims 19-27 were rejected under 35 U.S.C. §101, because the "computer readable medium" was associated in the written description with "transmission media" in the form or "waves or signals." Respectfully, this rejection is traversed. The preamble of the claim recites a "computer program product in a computer readable medium," and such a medium is a "manufacture" within the meaning of 35 U.S.C. §101. Accordingly, the Examiner is requested to reconsider and withdraw this rejection.

Claims 1, 10 and 19 were rejected under 35 U.S.C. §112, 2nd paragraph, because the "from servers" phrase was considered indefinite. This rejection has been addressed by removing this phrase from each such claim, as the phrase was superfluous (because a "cookie" associated with a "domain identifier" is generated from a server). The function as now recited merely indicates that "the parameters comprise domain identifiers associated with indications of whether to block transmission of cookies associated with the domain identifiers."

Claim 6 stands rejected under 35 U.S.C. §112, 1st paragraph, as failing to comply with the enablement requirement, because the phrase "multiple sets of parameters" is alleged to be unclear. Respectfully, this rejection is traversed. The "multiple sets of parameters" phrase (identified on page 5, lines 19-20, and in the Abstract) is simply a shorthand reference to the "client profile" filtering aspect of the invention, where, in addition to the primary feature disclosed (namely, user-configurable cookie filtering on a per-domain basis), a user also can configure multiple "client profiles" at the proxy server. As illustrated in FIG. 6B, a user thus may enable client profile filtering of cookies (on a per domain basis), and there is a "set of parameters" associated with a given client profile. This is evident from this sentence on page 24, line 30: "[t]he source domain filtering parameters that are associated with the current client profile." The "filtering parameters" are one set of parameters, and when two or more client profiles are available, there are then "multiple sets of parameters" within the meaning of claim 6. The claim is enabled by the written description, especially as the phrase in question was used in the original written description. The Examiner is asked to reconsider and withdraw this rejection.

Claims 1-27 were rejected under 35 U.S.C. §103(a) as being unpatentable over Grantges, Jr., U.S. Patent No. 6,324,648, in view of Datar et al, U.S. Patent No. 6,351,812, further in view of Rathbun et al, U.S. Publication No. 2003/0005308. Respectfully, this rejection is traversed, as the three references do not disclose or relate at all to filtering of cookies being returned from a server back to a requesting client. This is clear from an analysis of the "scope and content" of the prior art, which analysis is set forth below.

Grantges describes a system for provided authenticated access for a client over an insecure public network. Using a web browser, the client accesses an application gateway through a proxy server 34 having a plug-in 36. The proxy server intercepts message destined for a backend application and creates a cookie. The cookie contains an identifier sufficient to identify a destination server corresponding to the backend application. Subsequent messages from the client include the cookie. Upon receipt, the application gateway processes the cookie and, if valid, the gateway appends the identifier to a destination URL that identifies the destination server to enable the messages to be routed appropriately.

The Grantges patent does not disclose or suggest proxy server filtering of a cookie that is being returned from a server to a client, let alone per-domain cookie filtering.

Datar et al describes how a participant in an online electronic commerce transaction can validate his/her own certificate by accessing an authority that checks whether the participant's certificate is valid. If the certificate is valid, the authority passes back a cookie that includes a plurality of attributes descriptive of the certificate, namely, the identity of the certificate, a timestamp, the status of the certificate (not revoked, revoked, unknown) and, if revoked, revocation date, revocation reason, and the like, together with a digital signature of the attributes. When accessing a secure application, the participant then presents both the certificate and the cookie, obviating a real-time inquiry to the authority except in the event of a stale or missing cookie.

The Datar et al patent does not disclose or suggest proxy server filtering of a cookie that is being returned from a server to a client, let alone per-domain cookie filtering.

Rathbun et al describes a method and system for restricting client access to a web site. In this system, a first web server receives a client login and, in response, allocates a cookie to the client that contains an access credential having at least one client-based role-based attribute. A

second web server hosts the secured web site having an associated security file containing at least one client role-based access privilege. In response to the client's request at the second server, the cookie is retrieved and decoded, and the access credential is compared to the access privilege. If the credential has an attribute in common with the privilege, the client is granted access to the site.

The Rathbun et al patent application likewise does not disclose or suggest proxy server filtering of a cookie that is being returned from a server to a client, let alone per-domain cookie filtering.

As can be seen, each prior art reference simply deals with cookie generation, and then using the cookie to obtain access to some protected resource. This is not the subject matter of the claims here. Rather, the claims here assume that the client has obtained access to the server and that the server has issued the cookie. Unlike the cited art, the claims concern whether that cookie will be returned to the client. This "cookie filtering" concept is not disclosed or suggested by any of the art of record, as none of the references even address the question of how a cookie being returned from a server to the client should be processed, let alone filtered according to user-configurable options. In particular, the prior art does not describe providing a technique for enabling a user to configure per-domain (and, optionally, per-client profile) filtering of cookies that are returned from servers. Rather, the cited prior art deals with an unrelated issue, *viz*., how to process a cookie being passed from a client to the server.

Grantges, the primary reference, has been cited for its alleged teaching of "receiving at the proxy server a response message from the server for the client" and "detecting at the proxy server a cookie associated with the response message." In both cases the Examiner has pointed to this passage in Grantges: "[i]n step 214, DMZ proxy server 34 via programmed plug-in 36 determines whether the incoming message contains a valid authentication cookie (emphasis supplied)." Respectfully, the Examiner has erred here in reading the "incoming message" in Grantges as the "response message" described in the claims. They are the exact opposite. In particular, an "incoming message" is a message received from the web browser 22 in Grantges, whereas the "response message" in the claims is the message being returned to the client (from the server). Thus, in the first instance, the reference does not teach the requisite "receiving at the proxy server a response message…" nor can the reference teach detecting the cookie in any such

message. Thus, contrary to the Examiner's conclusion, the first two limitations in each of the independent claims are not present in this reference.

Datar et al., the secondary reference, has been cited for its alleged teaching of "extracting from the response message a domain identifier associated with the server," citing to this passage (at column 4, lines 16-22): "... if the status authority is part of a foreign domain and, therefore, cannot issue a Cookie for the application's domain. In this embodiment ..., the status server returns the response to the inquiring application and the application in turn, returns the response to the participant for caching." The passage, according to the Examiner, necessarily implies the extracting step because the "cookie issuing authority takes valid domain into consideration" and presumably (according to the Examiner) must extract the domain identifier to do so. Respectfully, the Examiner's position is overstated, as the passage does not indicate how the status server performs this operation or, more to the point, whether it extracts a domain identifier (so that, for example, the extracted domain identifier can be compared with a set of user-configurable domains). The Examiner goes on to argue that one of ordinary skill would combine Datar et al with Grantges "in order to for [sic] a participant in electronic commerce to validate his/her own certificate ...". In arguing that the references can and should be combined, the Examiner has cited a motivation (creating a cookie that includes certificate attributes, and use of that cookie) that is not relevant to any aspect of the subject matter disclosed and claimed here. In rejecting a claim, the "pertinence of each reference, if not apparent, must be clearly explained." 37 CFR 1.104(c)(2).

Moreover, while admitting that Grantges and Datar et al are "silent on retrieving a set of parameters" – and they are - the Examiner contends that Rathbun et al retrieves such a set, where the parameters are "domain identifiers associated with indications of whether to block transmission of cookies from servers associated with the domain identifiers." Rathbun et al has no such teaching. As noted above, Rathbun et al passes a cookie that includes an access credential having at least one client role-based attribute. At the server, that attribute is attempted to be matched against a role-based access privilege. If a match occurs, access to a protected resource is provided. As noted above, however, Rathbun et al say nothing about filtering a cookie that is being returned from the server back to the requesting client, let alone comparing an

extracted domain identifier against other "domain identifiers" (such as have been configured into the proxy server) to facilitate that filtering operation.

For the reasons set forth above, the combination of the cited art still fails to disclose at least the following steps of claim 1:

"extracting from the response message a domain identifier associated with the server;

retrieving a set of parameters, wherein the parameters comprise domain identifiers associated with indications of whether to block transmission of cookies associated with the domain identifiers; and

processing the cookie at the proxy server in accordance with the retrieved set of parameters and the extracted domain identifier."

As the prior art does not disclose "processing the cookie" in accordance with the "retrieved set of parameters and the extracted domain identifier." This user-configurable per-source domain "filtering" provides an enhanced privacy service that is neither disclosed nor suggested by the prior art. Thus, independent claims 1 (method), 10 (apparatus) and 19 (computer program product) describe patentable subject matter.

Dependent claims 2, 11 and 20 describe the cookie filtering steps more specifically and, in particular, the steps of blocking the cookie from transmission, caching the cookie at the proxy, and sending a modified response message to the client. This is the scenario such as described in steps 614, 618 and 620 of FIG. 6A, where the user has selected an option not to allow the cookie through the privacy service proxy server. These claims are separately patentable because the cited art does not teach any filtering of cookies being returned from a server to a client, let alone the specific requirements set forth in these claims.

Dependent claims 3, 12 and 21 likewise describe the cookie filtering steps but in this case describe the operation where the cookie (of a recognized domain) is passed back to the client. This is the scenario such as described in step 614 and 616 of FIG. 6A, where the user has selected an option to allow the cookie through the privacy service, in which case the privacy service sends the response to the client without removing or detaching the cookie from the response. These claims likewise are patentable over the cited references, which do not teach any response cookie filtering.

Dependent claims 4, 13 and 22 are separately patentable as they describe the additional functionality of "configuring the step of parameters" at the proxy server. In one illustrated embodiment, the user interfaces (FIGs. 4A-4C) can be used for this purpose. The cited art does not teach any user-configurable options, let alone for the cookie filtering functionality of the subject disclosure.

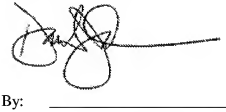
Dependent claims 5, 14 and 23 are separately patentable as they describe the further step of determining if the set of parameters contains an indication that the user has enabled cookie processing by the proxy server. In one embodiment, this refers to determining whether a "source domain filter enable flag" (218) is set. The cited art does not perform cookie filtering, so this functionality is also absent from any combination of the references.

Dependent claims 6, 15 and 24 are separately patentable as they describe the further steps of managing the "multiple set of parameters." This is the client profile option, as previously described. The references do not disclose or suggest cookie filtering on a per-domain basis, thus they cannot teach the further features recited in these claims.

Dependent claims 7-9, 16-18 and 25-27 are patentable for the reasons advanced with respect to their parent claims.

A Notice of Allowance is respectfully requested.

Respectfully submitted,



By: _____
David H. Judson, Reg. No. 30,467